



Department of Homeland Security Daily Open Source Infrastructure Report for 27 July 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Detroit Free Press reports Northwest Airlines on Wednesday, July 26, was still trying to fix a computer problem that started Tuesday and delayed 285 flights at Detroit Metro Airport, as well as at Minneapolis/St. Paul and Memphis hubs. (See item [18](#))
- Investigators say when two planes almost collided on Sunday night, July 23, at Chicago's O'Hare International Airport, the alarm that is supposed to prevent that from happening was switched off. (See item [19](#))
- Reuters reports GlaxoSmithKline says a bird flu vaccine for humans that uses only a very low dose of active ingredient has proved effective in clinical tests and could be mass-produced in 2007. (See item [27](#))
- The Department of Homeland Security on Wednesday, July 26, announced a new initiative and best business practices to help employers ensure they are building a legal workforce through voluntary partnerships with the government. (See item [31](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *July 26, New York Times* — **All in Queens have power now, Con Ed says.** Consolidated Edison (Con Ed) said Wednesday, July 26, that it had restored electricity to all the customers who endured a blackout in an eight-square-mile chunk of northwest Queens for more than a week. Joy Faber, company spokesperson, said that some customers in the area may still experience low voltage or occasional outages. Con Ed estimated that at its worst, the blackout affected about 25,000 customers, but a “customer,” to the utility company, can be anything from a one-family house to a large apartment building. The rule of thumb is to figure that there are four people for every “customer,” so at the height of the blackout 100,000 people were without lights, elevators and air-conditioning during one of the hottest weeks of the year. Con Ed spokesperson Michael Clendenin said low-voltage lines in the street were knocked out when 10 feeder cables, each carrying up to 27,000 volts, failed, causing the blackout. The low-voltage lines connect to the lines running directly into homes or businesses. Mayor Michael R. Bloomberg said that replacement feeder cables, installed above the ground as a stopgap measure during the blackout, need to be buried. He said the utility would leave its emergency generators in affected neighborhoods.
Source: <http://www.nytimes.com/2006/07/26/nyregion/26cnd-power.html?hp&ex=1153972800&en=08cd591ce59c0b3f&ei=5094&partner=homepag e>
2. *July 26, Washington Post* — **Deadly heat continues in California; slight cooling trend this week may ease blackout concerns.** California edged away from mandatory electricity blackouts Tuesday, July 25, as slightly cooler air — although still in the low 100s — began to filter across much of the state. A day after the state shattered its record for electricity consumption, power managers said clouds and lower temperatures in coming days would lessen the likelihood of rolling blackouts. A power emergency on Monday, July 24, required some businesses to curtail power use in exchange for lower electricity rates. It has ended, although residents were being warned to conserve power and limit the use of large appliances during daytime hours. More than 50,000 homes and businesses were without power Tuesday. The aging electricity-transmission grid in and around Los Angeles — some of it built in the 1920s and 1930s — could not handle the spiking power demands that came with persistent high temperatures. “Transformer failure was driven by the prolonged heat wave, which since July 13 has meant that they cannot cool down at night,” said Ron Litzinger of Southern California Edison. The heat wave comes at a time when ambient year-round temperatures in Southern California are on the rise.
Source: <http://www.washingtonpost.com/wp-dyn/content/article/2006/07/25/AR2006072501297.html>
3. *July 26, Associated Press* — **Nigerian oil pipeline springs leak.** Oil multinationals in Nigeria have shut off 210,000 barrels of daily crude production after an unexplained leak on a shared pipeline, oil industry officials said Tuesday, July 25. It was not immediately known what caused the leak in the line used by Royal Dutch Shell PLC and ChevronTexaco Corp. Don Campbell of ChevronTexaco said the leak in the shared pipeline was costing his company 30,000 barrels per day. The pipeline was shut down over the weekend. Nigeria is Africa's largest oil exporter and the fifth-largest supplier of crude to the United States. The country produces about 2.5 million barrels of oil daily. With the leak, Shell has shut off a total of 653,000 barrels per day in production.
Source: http://www.cnn.com/2006/WORLD/africa/07/25/nigeria.pipeline.ap/index.html?section=cnn_latest

4. *July 20, Federal Energy Regulatory Commission* — **Long-term transmission rights guidelines finalized.** The Federal Energy Regulatory Commission (FERC) Thursday, July 20, finalized guidelines for independent transmission organizations to follow in developing proposals to provide long-term firm transmission rights in organized electricity markets. These guidelines will increase long-term transmission price certainty in the organized electricity markets and allow for new investments and other long-term power supply arrangements, the Commission said. The Commission noted that the guidelines adopted in the final rule "will give transmission organizations the flexibility to propose designs for long-term transmission rights that reflect regional preferences and accommodate their regional market designs..." The final rule requires independent transmission organizations such as Regional Transmission Organizations and Independent System Operators that oversee organized electricity markets to make long-term firm transmission rights available to all transmission customers. The availability of such rights will provide an added measure of certainty to load-serving entities that wish to enter into long-term power supply arrangements to serve their load, which in turn should allow load-serving entities to more readily obtain financing for new infrastructure. Source: <http://www.ferc.gov/press-room/press-releases/2006/2006-3/07-20-06-E-2.asp>

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[\[Return to top\]](#)

Defense Industrial Base Sector

5. *July 25, Government Accountability Office* — **GAO-06-981T: DoD Excess Property: Control Breakdowns Present Significant Security Risk and Continuing Waste and Inefficiency (Testimony).** In light of the Government Accountability Office's (GAO) past three testimonies and two reports on problems with controls over excess Department of Defense (DoD) property, GAO was asked to perform follow-up investigations to determine if (1) unauthorized parties could obtain sensitive excess military equipment that requires demilitarization (destruction) when no longer needed by DoD and (2) system and process improvements are adequate to prevent sales of new, unused excess items that DoD continues to buy or that are in demand by the military services. GAO briefed DoD management on the results of its follow-up investigation and provided additional perspectives on ways to resolve the control breakdowns that resulted in public sales of sensitive excess military equipment and new, unused excess items that the military services continue to use. In its comments on GAO's draft report, DoD stated that given the time allotted to comment, the department was not able to do a detailed review and has no comments at this time. DoD also commented that it continues to implement changes to procedures based on GAO's May 2005 report (GAO-05-277). Highlights: <http://www.gao.gov/highlights/d06981thigh.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-981T>

6. *July 25, Government Accountability Office* — **GAO-06-983T: DoD's High-Risk Areas:**

Challenges Remain to Achieving and Demonstrating Progress in Supply Chain

Management (Testimony). The Department of Defense (DoD) maintains a military force with unparalleled logistics capabilities, but it continues to confront decades-old supply chain management problems. The supply chain can be the critical link in determining whether our frontline military forces win or lose on the battlefield, and the investment of resources in the supply chain is substantial. Because of weaknesses in DoD's supply chain management, this program has been on the Government Accountability Office's (GAO) list of high-risk areas needing urgent attention and transformation since 1990. Last year, DoD developed a plan to resolve its long-term supply chain problems in three focus areas: requirements forecasting, asset visibility, and materiel distribution. In October 2005, GAO testified that the plan was a good first step. GAO was asked to provide its views on DoD's progress toward (1) implementing the supply chain management improvement plan and (2) incorporating performance measures for tracking and demonstrating improvement, as well as to comment on the alignment of DoD's supply chain management improvement plan with other department logistics plans. This testimony is based on prior GAO reports and ongoing work in this area. Highlights: <http://www.gao.gov/highlights/d06983thigh.pdf>
Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-983T>

[\[Return to top\]](#)

Banking and Finance Sector

7. *July 26, CNET News* — **System glitches hit two banks' online services.** Two of the nation's banks struggled on Tuesday, July 25, to repair glitches at their Websites that had prevented customers from fully accessing their accounts for as long as two days. Emigrant Direct, a bank recently written up in the Wall Street Journal and the New York Times for offering high-paying savings accounts, saw a malfunction block customers from entering the site for long stretches over a two-day period, according to a bank employee and customers who posted complaints at an Internet message board. Seattle-based Washington Mutual saw a systems defect prevent some customers from performing banking chores, according to the bank's representative. Customers of the financial services company who e-mailed CNET News.com said the problems began appearing over the weekend.
Source: http://news.com.com/System+glitches+hit+two+banks+online+services/2100-1047_3-6098492.html?tag=nefd.top
8. *July 26, Government Accountability Office* — **GAO-06-674: Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data (Report).** The growth of information resellers — companies that collect and resell publicly available and private information on individuals — has raised privacy and security concerns about this industry. These companies collectively maintain large amounts of detailed personal information on nearly all American consumers, and some have experienced security breaches in recent years. The Government Accountability Office (GAO) was asked to examine (1) financial institutions' use of resellers; (2) federal privacy and security laws applicable to resellers; (3) federal regulators' oversight of resellers; and (4) regulators' oversight of financial institution compliance with privacy and data security laws. To address these objectives, GAO analyzed documents and interviewed representatives from 10 information resellers, 14 financial institutions, 11 regulators, industry and consumer groups, and others. Congress should consider

(1) requiring information resellers to safeguard all sensitive personal information they hold, and
(2) giving the Federal Trade Commission civil penalty authority for enforcement of the Gramm–Leach–Bliley Act's (GLBA) privacy and safeguarding provisions. GAO also recommends that state insurance regulators ensure compliance with GLBA.

Highlights: <http://www.gao.gov/highlights/d06674high.pdf>

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-06-674>

9. *July 25, Tech World* — Report: Crypto malware close to being uncrackable.

File–encrypting Trojans are becoming so complex that the security companies could soon be powerless to reverse their effects, Kaspersky Lab has said in a new report, entitled *Malware Evolution: April – June 2006, Hidden Wars*. Commonly termed "ransomware," Trojans that encrypt data files on a user's PC before demanding a payment in return for supplying the key to unlock the files, have come from nowhere in recent months to become a measurable problem. Aleks Gostev of Kaspersky Lab raised the alarming possibility that victims could at some point in the near future have their files encrypted in such a way that the security industry would not be able to issue a fix. If this comes to pass -- and Kaspersky's claims that the day is not far off are plausible -- it will mark an important moment for the whole software security industry.

To view the report: <http://www.viruslist.com/analysis?pubid=191951869>

Source: <http://www.techworld.com/security/news/index.cfm?newsID=6507&pagtype=samechan>

10. *July 25, Lancaster Online (PA)* — Armstrong employee data stolen. A laptop computer containing a copy of information about 12,000 current and former Armstrong World Industries employees has been stolen. In a letter dated Thursday, July 20, Armstrong said the information was on a laptop taken from the locked car of a Deloitte & Touche employee who was auditing Armstrong's payroll. The information includes names, home addresses, home phone numbers, employee identification numbers, Social Security numbers and pay. The two–page letter adds that the company, as of Thursday, is not aware of any misuse of the data.

Source: <http://local.lancasteronline.com/4/24302>

11. *July 25, Tech Web* — Trojan spoofs Firefox extension, steals IDs. An identity–stealing keylogger that disguises itself as a Firefox extension and installs silently in the background was discovered Tuesday, July 25, by security vendor McAfee. According to the company, the "FormSpy" Trojan horse monitors mouse movements and key presses to steal online banking or credit card usernames and passwords, other login information, and URLs typed into Firefox. Another component of the Trojan sniffs out passwords from ICQ and FTP sessions, and IMAP and POP3 traffic, said McAfee. All collected information is sent to an IP address hard–coded into the Trojan. The scam starts with spam posing as a message from the billing support department of mega–retailer Wal–Mart, said Craig Schmugar, the virus research manager at McAfee's Avert Labs. "There's an order number in the message, which matches the number of the attachment," said Schmugar. "When someone opens the attachment, the Trojan downloads and installs two components, a keylogger as well as a sniffer."

Source: http://www.techweb.com/wire/security/191101268;jsessionid=WA_XIDIUIT1ZIQSNDLRCKHSCJUNN2JVN

12. *July 24, Computer World* — IRS warns of new e–mail scam. The Internal Revenue Service (IRS) is warning taxpayers of an e–mail scam that uses the Department of the Treasury's

Electronic Federal Tax Payment System (EFTPS) to lure them into disclosing personal information. The IRS said the e-mail scam is the first to target the EFTPS. The fake e-mail, which contains numerous grammatical and typographical errors, looks like a page from the IRS Website and claims to be from the "IRS Antifraud Commission," a fictitious group. The e-mail claims that someone has enrolled the taxpayer's credit card in EFTPS and has tried to pay taxes with it. It also says that there has been fraudulent activity involving the taxpayer's bank account and that the money was lost and "remaining funds" are blocked. Recipients are asked to click on a link that purports to help them recover their money, but the link takes them to a fake IRS site where they are asked to divulge personal information.

Source: <http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=government&articleId=9001961&taxonomyId=13>

[[Return to top](#)]

Transportation and Border Security Sector

13. *July 26, Associated Press* — **Jetliner loses engine, lands safely in NYC.** A Boeing 777 jetliner carrying more than 250 people lost power in one of its two engines Wednesday, July 26, but landed safely at New York's John F. Kennedy International Airport less than a half hour after the engine failed, said American Airlines spokesperson Billy Sanz. Officials were investigating what caused the problem on Flight 134. The plane was en route to London from Los Angeles. Sanz said all the passengers would be put on another plane.

Source: http://www.usatoday.com/travel/flights/2006-07-26-engine-fai lure_x.htm

14. *July 26, New York Times* — **FAA redirects air traffic controllers.** The Federal Aviation Administration (FAA) has rescheduled air traffic controllers at seven of its busiest radar offices to assure that at least 70 percent of the controllers on shift are always at their radar scopes. The agency hopes that the change will cut costs and errors. But controllers say that they are working without breaks longer than rules allow and that their supervisors have lost the flexibility to assign rest periods based on how hectic a job has been. The controllers union has filed several grievances relating to the change, the latest result of an agency campaign to cut labor costs. The schedule change covers Terminal Radar Approach Controls, known as Tracons, which generally handle traffic on approach to airports or on departure, and at low altitude. It applies to New York, Northern California, Southern California, Dallas/Fort Worth, Atlanta, Chicago, and the Washington, DC area. Several conditions of controller employment recognize the level of concentration the job requires. For example, controllers must retire at age 56. Controllers also argue that handling more traffic and then having a slightly longer break is safer.

Source: <http://www.nytimes.com/2006/07/26/washington/26air.html?ref=us>

15. *July 26, Boston Globe* — **Stability of Boston tunnel ramps' massive fans in question.** Massachusetts state transportation officials said on Tuesday, July 25, they were concerned about the stability of five massive jet fans suspended above two Big Dig ramps, the latest in a growing list of potential problems that threaten to further snarl Boston's traffic. State transportation officials said they would inspect the five jet fans, at least two of which are anchored by epoxy-secured bolts. One uses a stronger anchoring system, and state inspectors are uncertain what holds up the other two. State officials said the discovery of another safety threat underscores the inadequacy of inspections conducted by the Massachusetts Turnpike

Authority in the days after Milena Del Valle was killed July 10, by falling concrete ceiling panels in the Interstate 90 connector tunnel. After the ceiling collapse, Turnpike Authority inspectors examined the ramps and the Ted Williams Tunnel, but failed to identify the multi-ton fans as a possible problem and missed three loose ceiling bolts in the Ted Williams Tunnel, which were detected when state transportation engineers conducted their own inspections. Because of the lengthening list of problems, Governor Mitt Romney and other state officials have backed away from once-confident forecasts of reopening.

Source: http://www.boston.com/news/traffic/bigdig/articles/2006/07/26/stability_of_ramps_massive_fans_in_question/

16. *July 26, Associated Press* — **Airline fires pilot removed from flight.** A Continental Airlines captain removed from a flight because another employee smelled alcohol on his breath was fired Tuesday, July 25, the airline said. The pilot, who was not identified, tested above the legal limit for alcohol for pilots, and was dismissed two days after being removed from the aircraft on suspicion of intoxication, said Sarah Anthony, a Continental spokesperson. The pilot was scheduled for Flight 706, from George Bush Intercontinental Airport to Tampa, on Sunday, July 23. It was his first flight of the day.

Source: http://www.usatoday.com/travel/flights/2006-07-26-continental-pilot_x.htm

17. *July 26, USA TODAY* — **Honda's microjet starting this fall.** Honda, the Japanese carmaker, said Tuesday, July 25, it will begin selling aircraft starting this fall. Dubbed HondaJet, it becomes the latest entrant in what is expected to be a competitive market for "very light jets," or VLJs. The very light jets, typically seating eight or fewer passengers, are vying for the most coveted of air travelers — the very wealthy and those corporate executives willing and financially able to bypass traditional commercial airlines. According to the Federal Aviation Administration, about 4,500 microjets will be flying by 2016. Honda projects it will be three to four years before the FAA certifies its jet and it can begin flying. Honda plans to form an alliance with Vero Beach, FL-based Piper Aircraft to collaborate on sales and service and to explore opportunities in engineering and other areas in general and business aviation.

Source: http://www.usatoday.com/travel/news/2006-07-25-hondajet_x.htm

18. *July 26, Detroit Free Press* — **NWA flight delays continue after computer glitch.** Northwest Airlines on Wednesday, July 26, was still trying to fix a computer problem that started Tuesday afternoon and shut down many of the airline's check-in systems at Detroit Metro Airport. The airline's hubs at Minneapolis/St. Paul and Memphis — along with several other airports — were also affected, but to a lesser extent, according to Northwest spokesperson Kurt Ebenhoch. The airline was making progress on restoring the system. The network crash delayed 285 of its 1,364 flights on Tuesday, July 25. The airline expects to operate its full schedule Wednesday, which will be 1,364 flights. As of 11:10 a.m. EDT, there were no cancellations due to the computer problem, Ebenhoch said. But there have been delays.

Source: http://www.freep.com/apps/pbcs.dll/article?AID=/20060726/NEW_S99/60726008

19. *July 26, CBS Chicago* — **Alarm off during O'Hare close call.** Investigators say when two planes almost collided on Sunday night, July 23, at Chicago's O'Hare International Airport, the alarm that is supposed to prevent that from happening was switched off. Preliminary reports say United Flight 1015, which was bound for Denver, came within 200 feet of colliding with a cargo plane. A Federal Aviation Administration (FAA) representative said the alarm was shut

off because the agency is enhancing the system, and training controllers on how to use the upgrades. Meanwhile, the head of a union representing air traffic controllers says staffing shortages and the FAA are to blame. The FAA has said the controller should have monitored the situation more closely. The United Airlines flight was departing about 10 p.m. CDT Sunday when it flew over a Boeing 747 cargo plane that had just landed on an intersecting runway. An Atlas Air 747 landed on runway 14 right. It crossed the intersection of runway 27 left. That's where United Flight 1015 was just taking off.

Source: http://cbs2chicago.com/topstories/local_story_207081204.html

20. *July 25, USA TODAY* — **NTSB concerned rules don't apply to aging planes.** Planes like the aging seaplane that lost a wing and crashed in Miami in December, killing all 20 people aboard, won't be subject to new federal rules designed to protect the safety of older aircraft. The National Transportation Safety Board (NTSB) accused federal aviation regulators Tuesday, July 25, of ignoring a mandate from Congress by exempting all airline planes with fewer than 30 seats from regulations that will require additional inspections of aging planes. As planes age, metal weakens, and wiring becomes more susceptible to short-circuiting. Congress passed the Aging Airplane Safety Act in 1991, which required the Federal Aviation Administration (FAA) to mandate improved inspections and maintenance. Last year, when the FAA issued regulations ordered by the law, it exempted planes with fewer than 30 passenger seats. It also exempted planes designed before 1958. "The safety board is concerned that the exemptions ... exclude airplanes such as the accident airplane," the NTSB said in a letter sent to the FAA. "The FAA will certainly take a hard look at the NTSB's recommendations and respond to the board as quickly as possible," said Alison Duquette, FAA spokesperson. The FAA has issued more than 700 directives designed to improve safety on older planes, she said.

Source: http://www.usatoday.com/travel/flights/2006-07-25-ntsb-aging-planes_x.htm

[\[Return to top\]](#)

Postal and Shipping Sector

Nothing to report.

[\[Return to top\]](#)

Agriculture Sector

21. *July 26, Associated Press* — **Heat causes pileup of livestock carcasses.** California's record-setting heat wave has killed thousands of dairy cows and other livestock, leaving farmers with piles of carcasses and creating a backup at factories that turn the dead animals into pet food. A combination of sweltering temperatures, growth in the state's five billion dollar dairy industry and fewer plants to properly dispose of the animals have forced several counties to declare a state of emergency. The declarations allow dead livestock to be dumped in landfills – something usually outlawed because of health risks. Fresno County, which reached 113 degrees in recent days, was one of the first to declare an emergency when a plant that handles the bulk of the region's dead animals broke down earlier this month. After the old carcasses began decomposing in the searing summer heat, county officials were forced to make the declaration. San Joaquin County, which also has declared an emergency, estimated that its dairy

farms were losing a total of 120 cows per day from the heat. Individual dairy farmers could lose about two percent of their herd this year, according to industry experts. Hundreds of thousands of chickens and turkeys also have died.

Source: http://hosted.ap.org/dynamic/stories/D/DEAD_LIVESTOCK?SITE=7219&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2006-07-26-03-19-01

22. *July 25, Stop Soybean Rust News* — Soybean rust found in three sentinel plots in Florida.

Florida officials say soybean rust was found on three sentinel soybean plots in Gadsden County in north central Florida. These sites were located within three miles of an infected kudzu site. Georgia officials reported Monday, July 24th, a soybean rust find on soybeans in Brooks County. The two previous finds in this county have been on kudzu. Currently rust has only been found on this year's soybeans in five different counties in three states (Alabama, Florida and Georgia), the rest of the finds have been on kudzu. A total of 25 counties have reported rust this year and include five in Alabama, 12 in Florida, five in Georgia, two in Louisiana, and one in Texas.

Source: <http://www.stopsoybeanrust.com/viewStory.asp?StoryID=889>

[[Return to top](#)]

Food Sector

23. *July 26, Associated Press* — Japan to lift U.S. beef ban. The Japanese government will officially approve resuming U.S. beef imports from selected meat processing plants on Thursday, July 27, easing a blanket ban imposed earlier this year over mad cow fears, officials said. The approval will come after a strategy meeting of the Agriculture ministry on Thursday, where officials will debate when to start accepting beef shipments and other details, according to ministry official Hiroaki Ogura. The ruling Liberal Democratic Party agreed Wednesday, July 26, to resume imports from selected facilities after being briefed by government officials on a recent inspection tour of U.S. meat-processing plants. Japanese inspectors toured 35 plants to find out whether they meet Japanese guidelines against mad cow disease, or bovine spongiform encephalopathy. Under a bilateral agreement, all beef shipped to Japan must come from cattle less than 20 months old and no brain or spinal material can be included because that tissue is known to carry the disease. Inspectors found problems at one of the 35 plants, and the facility will not be immediately allowed to resume exports, Kyodo News agency reported. Public broadcaster NHK said a second facility would remain under surveillance because it was found to have previously broken import rules.

Source: <http://www.chron.com/disp/story.mpl/ap/fn/4072802.html>

24. *July 25, Food Safety and Inspection Service* — Hot dogs recalled. Ramar Foods Corp., a Pittsburg, CA, firm, is voluntarily recalling hot dogs that may be contaminated with *Listeria monocytogenes*, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, July 25. The hot dogs were produced on July 17, 2006 and were distributed to a retail outlet in San Leandro, CA. The problem was discovered through FSIS microbiological testing. FSIS has received no reports of illnesses associated with consumption of this product. Consumption of food contaminated with *Listeria monocytogenes* can cause listeriosis, an uncommon but potentially fatal disease.

Source: http://www.fsis.usda.gov/News_&_Events/Recall_023_2006_Release/index.asp

25. *July 25, Food Safety and Inspection Service* — **Frozen meat loaf entrees recalled.** Nestlé Prepared Foods Company, a Gaffney, SC, establishment, is voluntarily recalling approximately 48,588 pounds of frozen meat loaf entrees that may contain pieces of plastic, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Tuesday, Jul 25. The frozen entrees were produced on May 3, and were distributed to retail establishments nationwide. The problem was discovered after the company received consumer complaints. FSIS has received no reports of injury from consumption of these products. Source: http://www.fsis.usda.gov/News_&_Events/Recall_022_2006_Release/index.asp

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

26. *July 26, All Headline News* — **Thailand confirms bird flu death.** The government of Thailand confirmed on Wednesday, July 26, that a teenage boy died of bird flu. Health officials said the boy caught the virus from one of his fighting cocks in northern Thailand. Authorities said he was a 17-year-old from Pichit province. Health officials confirmed a fresh outbreak of the deadly H5N1 strain of the virus in Pichit. The chief of Pichit's disease control department, Thawat Suntrajarn said the boy died from a combination of dengue fever and bird flu which was common in people who succumbed from the H5N1 virus strain. He said the boy consulted a doctor last week and died Monday, July 24. Bangkok has dispatched 20 veterinarians in Pichit to contain the outbreak and banned all movements of poultry in the province. Seven other provinces were put on high alert. Source: <http://www.allheadlinenews.com/articles/7004333948>

27. *July 26, Reuters* — **Bird flu vaccine seen ready in 2007.** A bird flu vaccine for humans that uses only a very low dose of active ingredient has proved effective in clinical tests and could be mass-produced in 2007, its maker GlaxoSmithKline Plc said on Wednesday, July 26. Europe's biggest pharmaceuticals group said it was on track to start manufacturing by the end of 2006 and could make hundreds of millions of doses next year, assuming the product is approved by regulators. Companies are racing to develop pandemic H5N1 vaccines that could save lives and buy time to develop a vaccine against a pandemic strain. It could take from four to six months from the start of a pandemic before a specific vaccine will be ready. Other firms working on a bird flu vaccine include Novartis AG and Baxter International Inc. Source: http://today.reuters.com/news/newsArticle.aspx?type=businessNews&storyID=2006-07-26T092227Z_01_L26693955_RTRUKOC_0_US-BIRDFLU-GLAXO-VACCINE.xml&archived=False

28. *July 25, Agence France-Presse* — **West African health ministers to meet in Nigeria.** West African health ministers will meet in the Nigerian capital Abuja Thursday, July 27, to discuss

the latest developments in the avian flu and polio epidemics which have ravaged some parts of the region, an official statement said. The seventh ordinary meeting of the assembly of health ministers of the West African Health Organization (WAHO) will also consider a reproduction health commodity security strategy for the region, the Economic Community of West African States (ECOWAS) said Tuesday, July 25. It will consider the reports of a committee of health experts on the avian flu and polio epidemics in the region and the reduction of taxes and tariffs on drugs for malaria control.

Source: http://news.yahoo.com/s/afp/20060725/hl_afp/africahealthnigeria_060725193350: ylt=Ah0HvHVlB7N4xermCInRFh.JOrgF: ylu=X3oD MTA5aHJvMDdwBHNIYwN5bmNhdA--

29. *July 25, University of California–San Diego School of Medicine* — **Irradiation preserves T–Cell responses in bacterial vaccine.** Using gamma radiation to inactivate bacteria for the preparation of vaccines, instead of traditional heat or chemical methods of inactivation, appears to create a vaccine that is more effective than so-called “killed” vaccines against disease, and has the added advantage of a longer storage life than “live” vaccines, according to researchers at the University of California, San Diego (UCSD) School of Medicine. Their findings could result in more potent vaccines that are relatively inexpensive to produce, easy to store, and that can be transported without refrigeration. In experiments with mice, the researchers demonstrated that a vaccine made with irradiated *Listeria monocytogenes* (LM) bacteria provided much better protection against disease than vaccine made from heat-killed bacteria. *Listeria* is a food-borne pathogen that can cause severe meningitis and systemic illness in immuno-compromised individuals. To test the irradiated LM, mice were vaccinated with either heat-killed or irradiated vaccine, and then given lethal doses of LM bacteria. All of the unvaccinated or heat-killed vaccinated mice died, but 80 percent of those vaccinated with the irradiated vaccine survived. Protection against infection lasted more than one year after vaccination with irradiated LM.

Source: http://health.ucsd.edu/news/2006/07_25_Raz.htm

30. *July 24, Associated Press* — **Man staying at Colorado Air Force Academy camp dies from hantavirus infection.** A 58-year-old man staying at a campground for military personnel contracted hantavirus and died, Air Force Academy and state health officials said Friday, July 21. He died Wednesday, July 19, of the disease that is passed to humans when they inhale particles of dried urine or feces from infected rodents, officials said. He and his wife had been staying at the Peregrine Pines FamCamp, located in a wooded area between the academy’s Falcon Stadium and Interstate 25, for several months. “He was ill for about four days with fever and aches and over the weekend started developing some respiratory involvement,” said John Pape an epidemiologist with the Colorado Department of Public Health and Environment. There is no drug treatment for hantavirus. Academy officials inspected the campground and others for evidence of rodent droppings and have no plans to close the campground. No other cases have been reported at the school near Colorado Springs, CO. There have been 48 cases of hantavirus in Colorado between 1993 and 2005 and fewer than 450 cases have been recorded nationwide.

Hantavirus information: <http://www.cdc.gov/ncidod/diseases/hanta/hps/index.htm>

Source: <http://www.airforcetimes.com/story.php?f=1-292925-1974099.ph p>

Government Sector

31. *July 26, Department of Homeland Security* — **DHS highlights best practices for maintaining legal workforces.** The Department of Homeland Security (DHS) on Wednesday, July 26, announced a new initiative and best business practices to help employers ensure they are building a legal workforce through voluntary partnerships with the government. Called the ICE Mutual Agreement between Government and Employers (IMAGE), the program is designed to build cooperative relationships between government and businesses to strengthen hiring practices and reduce the unlawful employment of illegal aliens. The initiative also seeks to accomplish greater industry compliance and corporate due diligence through enhanced federal training and education of employers. As the criminal prosecution of worksite violations has increased in recent years, DHS has been flooded by requests from employers seeking information on how to avoid hiring illegal aliens. IMAGE is a balanced and carefully designed partnership program that seeks to provide answers to these questions and help employers comply with the law. Under this program, ICE will partner with companies representing a broad cross section of industries in order that these firms may serve as charter members of IMAGE and liaisons to the larger business community. To date more than 10,000 employers across the United States are using the Basic Pilot Employment Verification to check the work authorization of their newly hired employees.
Source: <http://www.dhs.gov/dhspublic/display?content=5757>

[[Return to top](#)]

Emergency Services Sector

32. *July 26, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** Tropical activity: Atlantic/Gulf of Mexico/Caribbean Sea: An elongated surface low pressure system over South Texas extending from near McAllen northeastward to Baffin Bay is producing a large area of showers and thunderstorms along with strong gusty winds in squalls over portions of the western Gulf of Mexico and the adjacent coastal areas. Radar and surface observations suggest that a low pressure center may be trying to form along the Texas coast near Baffin Bay. Upper-level winds are somewhat favorable for development and a tropical depression could still form if the low pressure system moves or develops farther to the east over the Gulf of Mexico. Regardless of whether a tropical cyclone forms this system will likely bring locally heavy rainfall to portions of the Texas Coastal Bend region the Upper Texas Coast and southern Louisiana during the next couple of days as it moves slowly northward.
Eastern Pacific: At 11:00 p.m. EDT Tuesday, July 25, 2006, Daniel was downgraded to a Tropical Storm.
Wildfire update: Heavy wildland fire activity was reported with 548 new fires reported. Twenty-one new large fires were reported: four in California, seven in Nevada, six in Oregon, three in Montana, and one in Washington.
Source: <http://www.fema.gov/emergency/reports/2006/nat072606.shtm>

33. *July 25, News Channel 3 (VA)* — **First responders in Hampton Roads, Virginia, meet to**

discuss hurricane preparedness. Dozens of first responders in Hampton Roads, VA, met Monday, July 24 and admitted that not everyone has a way to get out in the event of a hurricane emergency. Many cities are still working on getting those with special needs to safety. While it's clear there are a lot of bugs to be worked out, the meeting let the state know where each city stands and what it needs to get everyone out safely.

Source: <http://www.wtkr.com/Global/story.asp?S=5190195&nav=ZolHbyvj>

34. *July 24, Coloradoan (CO)* — **Disabled disaster preparedness on radar.** Nine years to the day of the flood in Fort Collins, CO, that killed five people and injured at least 400, a focus group will meet to discuss plans to locate and take care of the disabled and elderly population in case of another disaster in Larimer County. On Friday, July 28, organizations and Larimer County residents will discuss ideas of ways to contact people who live alone and might not be able to evacuate themselves in an emergency, said Susan Williams, chairwoman of the city's Commission on Disability. The county has no contact plan in place, Williams said. The group will focus primarily on how to contact people in case of natural disasters such as floods, fires and tornadoes or a breach at Horsetooth Dam.

Source: <http://www.coloradoan.com/apps/pbcs.dll/article?AID=/20060724/NEWS01/607240302/1002>

35. *July 19, Government Information Technology Agency* — **DHS border grant connects first responders in Arizona.** The WiFi First Responder Pilot Project has recently given emergency personnel high-speed access to the Internet along the CANAMEX Corridor near Arizona's southern border. This project allows first responders to connect to the Internet from their vehicles across a 30-mile stretch of I-19 from Green Valley in Pima County to Rio Rico in Santa Cruz County. The project showcases technological solutions to problems such as network security, and increased access to telecommunications for first responders and rural areas. Created by Congress in 1995, the CANAMEX Corridor is a series of highways connecting Mexico and Canada via rural areas in Arizona, Nevada, Utah, Idaho and Montana. In Arizona, the corridor is 487 miles long, and extends through long expanses of rural areas which lack reliable cellular and landline telecommunication services. The WiFi Pilot Project was funded by a grant from the Department of Homeland Security's (DHS) Information Technology and Evaluation Program to improve information sharing and integration among first responders.

Source: http://gita.state.az.us/tech_news/2006/7_19_06.htm

[[Return to top](#)]

Information Technology and Telecommunications Sector

36. *July 26, Security Focus* — **Mozilla Firefox, SeaMonkey, Camino, and Thunderbird multiple remote vulnerabilities.** The Mozilla Foundation has released thirteen security advisories specifying security vulnerabilities in Mozilla Firefox, SeaMonkey, Camino, and Thunderbird. Analysis: The vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application crash affected applications run JavaScript code with elevated privileges, potentially allowing the remote execution of machine code to gain access to potentially sensitive information.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/18228/info>

Solution: New versions of Firefox, SeaMonkey, Camino, and Thunderbird are available to

address these issues. Most Mozilla applications have self-updating features that may be used to download and install fixes.

Please see the referenced advisories for information on obtaining and applying fixes:

<http://www.securityfocus.com/bid/18228/references>

Source: <http://www.securityfocus.com/bid/18228/discuss>

37. *July 26, eWeek* — **Netscape.com hacked by Digg fans.** The ongoing Digg versus Netscape spat has apparently escalated into a hacking attack against America Online's Netscape.com social media Website. Virus researchers at Finnish security vendor F-Secure discovered the Netscape.com hack during research work around cross-site scripting vulnerabilities on social networking sites and said the attack was obviously the work of Digg fans.

Source: <http://www.eweek.com/article2/0.1895.1994528.00.asp>

38. *July 26, IDG News Service* — **Paris homes test very high-speed broadband.** France Télécom has laid new optical fiber connections direct to 100 homes in and around Paris to test a very high speed broadband access service, the company said Tuesday, July 25. For \$88 a month, customers participating in the fiber trial get Internet access, digital television broadcasts, and unlimited telephone calls over an optical connection with a theoretical maximum data rate of 2.5 Gbps downstream, and 1.2 Gbps upstream. Former monopoly operators in other countries are eyeing similar strategies. German operator Deutsche Telekom, for example, is laying fiber to the curb in front of German homes, and plans to use Very High Speed Digital Subscriber Line technology over the last few meters to deliver broadband services to the homes at up to 50 Mbps.

Source: http://www.infoworld.com/article/06/07/26/HNparishighspeed_1.html

39. *July 25, Security Focus* — **Microsoft Internet Explorer Native Function Iterator denial-of-service vulnerability.** Microsoft Internet Explorer is prone to a denial-of-service vulnerability. Analysis: This issue is triggered when an attacker convinces a victim user to visit a malicious Website. Remote attackers may exploit this issue to crash Internet Explorer, effectively denying service to legitimate users.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/19140/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/19140/references>

40. *July 25, Security Focus* — **Microsoft Windows remote denial-of-service vulnerability.** Microsoft Windows is reportedly prone to a remote denial-of-service vulnerability. Analysis: This issue may be due to the operating system's failure to properly handle unexpected network traffic. This issue may cause affected computers to crash, denying service to legitimate users.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/19135/info>

Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/19135/references>

41. *July 25, Sophos* — **Man faces 55 years in jail after charge of stealing 80,000 e-mail addresses.** Sophos has encouraged the authorities to continue to pursue the spamming community following the news that a man has been charged with stealing the membership database held at the American College of Physicians (ACP) in Philadelphia. William Bailey, Jr., of Charlotte, NC, faces a maximum possible sentence of 55 years in jail and \$2,750,000 in

finds if found guilty of illegally accessing the database and downloading contact details of 80,000 members of the ACP. Bailey runs a Website called dr-411.com, which sells professional organization member databases, including addresses and e-mail addresses for doctors, dentists, lawyers and real estate agents.

More information about the indictment can be found at:

<http://www.justice.gov/criminal/cybercrime/baileyCharge.htm>

Source: http://www.sophos.com/pressoffice/news/articles/2006/07/email_addresses_theft.html

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of active exploitation of a new vulnerability in Microsoft PowerPoint. Successful exploitation could allow a remote attacker to execute arbitrary code with the privileges of the user running PowerPoint.

For more information please review the following vulnerability note:

VU#936945: Microsoft PowerPoint contains an unspecified remote code execution vulnerability. <http://www.kb.cert.org/vuls/id/936945>

US-CERT strongly recommends the following until an update, patch, or more information becomes available:

Do not open attachments from unsolicited email messages.

Install anti virus software, and keep its virus signature files up to date.

Limit user privileges to no administrator rights.

Save and scan any attachments before opening them.

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. Users may wish to read Cyber Security Tip ST04-010 for more information on working with email attachments. <http://www.us-cert.gov/cas/tips/ST04-010.html>

US-CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.

http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 4672 (eMule), 50497 (---), 38566 (---), 65530 (WindowsMite), 12993 (---), 35830 (---), 24232 (---), 445 (microsoft-ds), 113 (auth) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	---

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[[Return to top](#)]

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[[Return to top](#)]

General Sector

Nothing to report.

[[Return to top](#)]

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open-source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983-3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282-9201.

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non-commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.